



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,364	07/17/2003	Colin John Blamires	03.028.01	8923
28875	7590	12/20/2010	EXAMINER	
Zilka-Kotab, PC			SIMITOSKI, MICHAEL J	
P.O. BOX 721120			ART UNIT	PAPER NUMBER
SAN JOSE, CA 95172-1120			2439	
		NOTIFICATION DATE	DELIVERY MODE	
		12/20/2010	ELECTRONIC	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

anita@zilkakotab.com  
dottie@zilkakotab.com  
jennifer@zilkakotab.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/620,364	<b>Applicant(s)</b> BLAMIRE ET AL.
	<b>Examiner</b> MICHAEL J. SIMITOSKI	<b>Art Unit</b> 2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 01 November 2010.  
 2a) This action is FINAL.      2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1,2,7-10,15-18 and 23-32 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_ is/are allowed.  
 6) Claim(s) 1,2,7-10,15-18 and 23-32 is/are rejected.  
 7) Claim(s) \_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 17 July 2003 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_

5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_

#### **DETAILED ACTION**

1. The response of 11/1/2010 was received and considered.
2. Claims 1-2, 7-10, 15-18 and 23-32 are pending.

#### **Response to Arguments**

3. Applicant's arguments with respect to claims 1-2, 7-10, 15-18 and 23-32 have been considered but are moot in view of the new ground(s) of rejection in view of Applicant's amendments.

#### **Claim Rejections - 35 USC § 103**

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-2, 7-10, 15-18, 23-25, 28-30 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,347,375 to Reinert et al. (**Reinert**) in view of U.S. Patent Application Publication 2003/0149887 to **Yadav**, Network Security Essentials, Applications and Standards by **Stallings** and U.S. Patent Application 2002/0199116 to Hoene et al. (**Hoene**).

Regarding claims 1 and 32, Reinert discloses a removable physical media (CD-ROM, col. 6, line 66) bearing a computer program (bootable virus utility, col. 6, lines 55-56) operable to control a computer to detect malware (viruses) by performing the steps of booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote

Art Unit: 2439

computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28), and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see

also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323). As modified, Reinert lacks wherein said removable physical media is operable such that security management code is automatically loaded and run from said removable physical media, and said security management code triggers said secure network connection using said network support code. However, Hoene teaches a system where a local virus scan occurs (¶27), where a client runs virus protector software, where the software establishes a connection to a server to obtain updated virus definitions prior to executing the virus scan. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert such that the security management code is automatically loaded and run from said removable physical media, and triggers said secure network connection using said network support code. One of ordinary skill in the art would have been motivated to perform such a modification to update the virus definitions prior to a local virus scan, as taught by Hoene.

Regarding claim 2, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 7, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 8, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 9, Reinert discloses booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6,

line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28) and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to

one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323). As modified, Reinert lacks wherein said removable physical media is operable such that security management code is automatically loaded and run from said removable physical media, and said security management code triggers said secure network connection using said network support code. However, Hoene teaches a system where a local virus scan occurs (¶27), where a client runs virus protector software, where the software establishes a connection to a server to obtain updated virus definitions prior to executing the virus scan. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert such that the security management code is automatically loaded and run from said removable physical media, and triggers said secure network connection using said network support code. One of ordinary skill in the art would have been motivated to perform such a modification to update the virus definitions prior to a local virus scan, as taught by Hoene.

Regarding claim 10, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 15, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 16, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 17, Reinert discloses a computer (computer 42, col. 7, line 60), said computer comprising a processor (CPU, col. 6, lines 39-40) performing the steps of booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28) and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have

been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44).

Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323). As modified, Reinert lacks wherein said removable physical media is operable such that security management code is automatically loaded and run from said removable physical media, and said security management code triggers said secure network connection using said network support code. However, Hoene teaches a system where a local virus scan occurs (¶27), where a client runs virus protector software, where the software establishes a connection to a server to obtain updated virus definitions prior to executing the virus scan. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert such that the security management code is automatically loaded and run from said removable physical media, and triggers said secure network connection using said network support code. One of ordinary skill in the art would have been motivated to perform such a modification to update the virus definitions prior to a local virus scan, as taught by Hoene.

Regarding claim 18, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 23, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 24, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 25, Reinert discloses a server computer (remote computer 54, col. 8, lines 10-11) connected by a network link to a computer (computer 42, Fig. 2), said server computer comprising a processor (inherent) configured to perform the steps of establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), loading one or more malware (virus) detection files (col. 8, lines 20-25) to said computer, wherein said computer is operable such that said computer is booted with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from a removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, wherein network support code (communications program) is loaded for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), wherein said computer is operable such that said network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said server computer (col. 7, lines 4-5 & lines 65-67), wherein malware detection is performed upon said computer using said one or more malware detection files (virus definition files, col. 8, line 10-11 & line 28). Reinert lacks the limitations “establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer”. However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a

signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323). As modified, Reinert lacks wherein said removable physical media is operable such that security management code is automatically loaded and run from said removable physical media, and said security management code triggers said secure network connection using said network support code. However, Hoene teaches a system where a local virus scan occurs (¶27), where a client runs virus protector software, where the software establishes a connection to a server to obtain updated virus definitions prior to executing the virus scan. Therefore, it would have been obvious to one having

Art Unit: 2439

ordinary skill in the art at the time the invention was made to modify Reinert such that the security management code is automatically loaded and run from said removable physical media, and triggers said secure network connection using said network support code. One of ordinary skill in the art would have been motivated to perform such a modification to update the virus definitions prior to a local virus scan, as taught by Hoene.

Regarding claim 28, Reinert discloses wherein said remote computer (remote computer 54) determines said one or more malware detection files that are downloaded to said computer (downloaded under the control of remote computer 54, col. 8, lines 10-25).

Regarding claim 29, Reinert discloses wherein said one or more malware detection files are determined based on said non-installed operating system (the malware detection files and service program must be able to run on the booted operating system, col. 8, lines 14-16 & lines 25-31).

Regarding claim 30, Reinert discloses wherein said one or more malware detection files (virus detection signature file) are determined based on a malware detection product (the virus detection signature file is used by the virus scanning software utility program, col. 8, lines 20-35).

6. Claims 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Reinert, Yadav, Stallings and Hoene**, as applied to claim 1 above, in further view of U.S. Patent 6,721,883 to Khatri et al. (Khatri).

Regarding claim 26, Reinert lacks wherein said computer is configured in its BIOS settings. However, Khatri teaches that computer systems boot from a specific device (col. 1, lines 16-17) by scanning through a boot order (col. 1, lines 35-39) that is determined by a BIOS setup routine (col. 4, lines 15-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to configure the BIOS settings to boot from said removable physical media. One of ordinary skill in the art would have been motivated to perform such a

Art Unit: 2439

modification to allow a modern computer system to boot from the CD-ROM of Reinert, as taught by Khatri (col. 1, lines 16-17, lines 35-39 & col. 4, lines 15-17).

Regarding claim 27, Reinert lacks wherein booting said computer with said non-installed operating system read from said removable physical media is based on a determination that a bootable removable media is present. However, Khatri teaches that computer systems boot from a specific device (col. 1, lines 16-17) by scanning through a boot order (col. 1, lines 35-39) such that the system attempts each device in a specific order (i.e. determines if each device can be boot from and boots from the first available, col. 1, lines 35-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Khatri to base the booting the computer with said non-installed operating system on a determination that the removable media is present. One of ordinary skill in the art would have been motivated to perform such a modification to use a standard computer boot order to boot from Reinert's CD-ROM, as taught by Khatri (col. 1, lines 16-17, lines 35-39 & col. 4, lines 15-17).

7. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Reinert, Yadav, Stallings and Hoene**, as applied to claim 1 above, in further view of U.S. Patent U.S. Patent 2003/0028889 to McCoskey et al. (**McCoskey**).

Regarding claim 31, Reinert lacks wherein said remote computer logs said downloading of said one or more malware detection files by said computer. However, McCoskey teaches a content delivery system such that when content is downloaded to a client, a delivery server logs the download so that billing servers can determine if the user will be charged a fee (¶126). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert's remote computer such that it logs the downloading of one or more malware detection files. One of

Art Unit: 2439

ordinary skill in the art would have been motivated to perform such a modification to allow a billing server to charge a fee for the download, as taught by McCloskey (¶126).

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 6, 2010  
/Michael J Simitoski/  
Primary Examiner, Art Unit 2439